RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: APP-M02

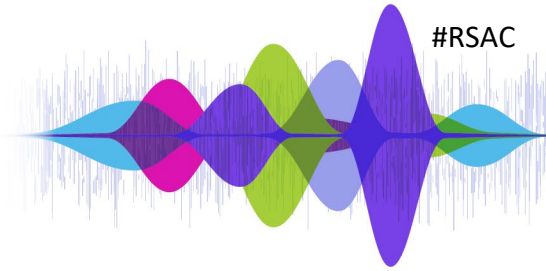
Secure by Design: Are We Winning?

Chris Wysopal

Founder & Chief Security Evangelist
Veracode
https://www.linkedin.com/in/wysopal/

Jason Healey

Senior Research Scholar
Columbia University SIPA
https://www.linkedin.com/in/jasonhealey/



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

RSAC 2025 Conference

Are we winning?

Measuring if Cyberspace Is Becoming More Defensible and Resilient

Many Voices.
One Community.

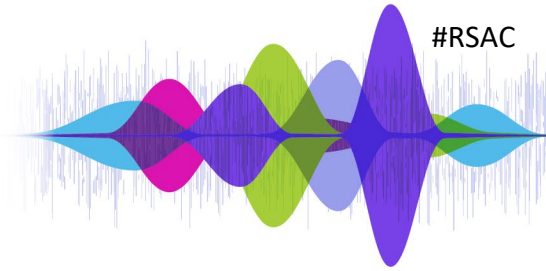
Defensive Struggles

- “Contemporary technology cannot provide a secure system in an open environment, which includes uncleared users working at physically unprotected consoles connected to the system by unprotected communications.”

- “None of the known [red] team efforts has failed to date.”

- “Few, if any, contemporary computer security controls have prevented a [red team] from easily accessing any information sought.”

Defensive Struggles



- “Contemporary technology cannot provide a secure system in an open environment, which includes uncleared users working at physically unprotected consoles connected to the system by unprotected communications.” 1970
- “None of the known [red] team efforts has failed to date.” 1972
- “Few if any contemporary computer security controls have prevented a [red team] from easily accessing any information sought.” 1979

Defensive Struggles

- "Contemporary technology cannot provide a secure system in an *open environment*, which includes uncleared users working at physically unprotected consoles connected to the system by unprotected communications." 1970

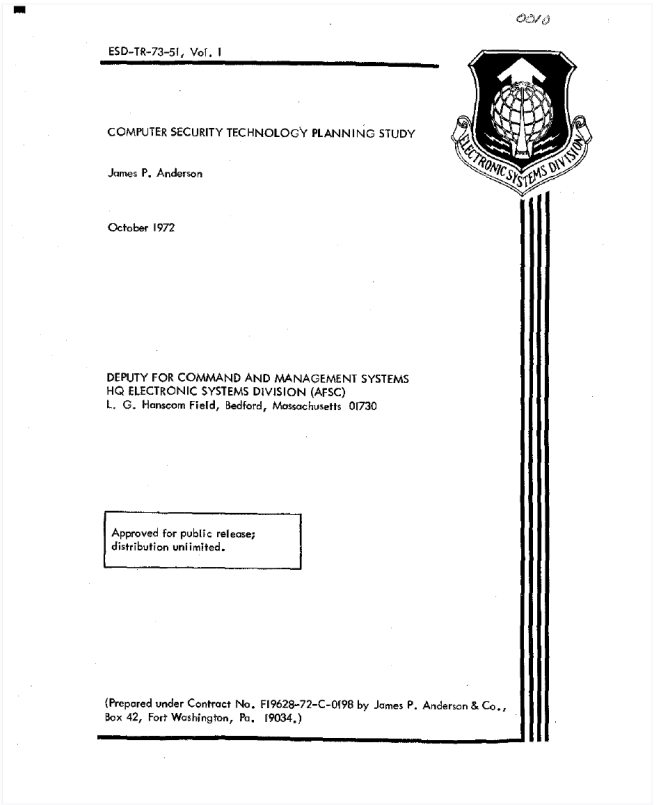
O>D

- "None of the known [red] team efforts has failed to date." 1972

- "Few if any contemporary computer security controls have prevented a [red team] from easily accessing any information sought." 1979

Secure By Design: Since 1972

- Securing “against the threat from a malicious user … is neither hopeless nor solved.”
- **“Unless security is designed into a system from its inception, there is little chance that it can be made secure by retrofit.”**
- “The reason that **an add-on approach, which looks so appealing, will not suffice** is that in order to provide defense against a malicious user, one must design the security controls into the operating system of a machine so as not only control the actions of each user, but of the many parts of the operating system itself when it is acting on a user’s behalf.”



ESD-TR-73-51, Vol. I

COMPUTER SECURITY TECHNOLOGY PLANNING STUDY

James P. Anderson

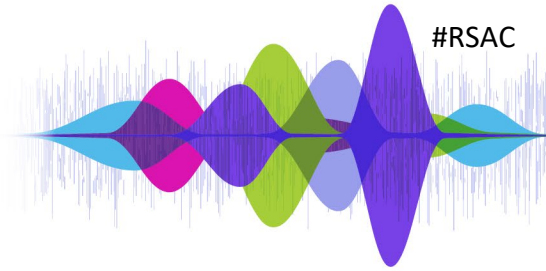
October 1972

DEPUTY FOR COMMAND AND MANAGEMENT SYSTEMS
HQ ELECTRONIC SYSTEMS DIVISION (AFSC)
L. G. Hanscom Field, Bedford, Massachusetts 01730

Approved for public release;
distribution unlimited.

(Prepared under Contract No. F19628-72-C-0198 by James P. Anderson & Co., Box 42, Fort Washington, Pa. 19034.)

What is Winning, Anyway?



Defenders Have *Supremacy*
Adversaries have tremendous difficulty achieving even simple goals against poorly resourced organizations

Attackers Have *Supremacy*
Even advanced defenders struggle to prevent basic attacks and threat attackers from achieving substantial impact

Defenders Have More *Advantages*
Adversaries can succeed but somewhat unpredictably and, generally, at high cost

Attackers Have More *Advantages*
Defense can succeed but somewhat unpredictably and, generally, at high cost

Defenders Are Winning

Adversaries Are Winning

D>>O D>O D=O D<O D<<O

What is Winning, Anyway?

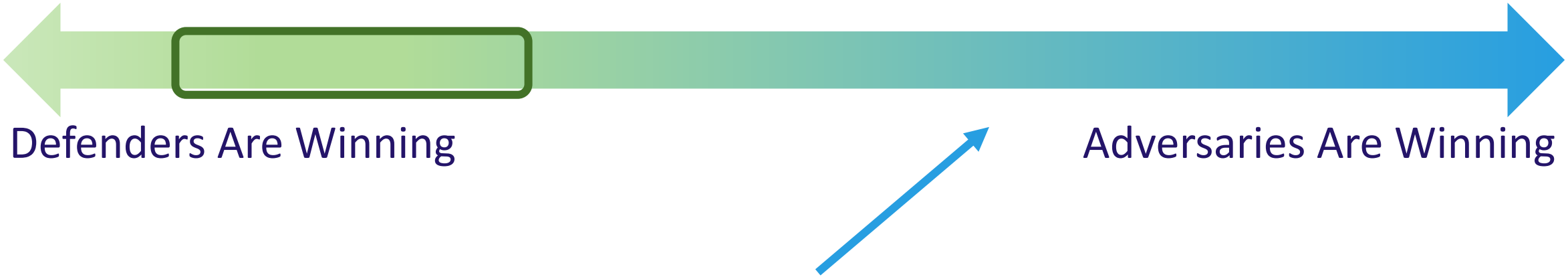
Before ~1970, we were around here

- Computers were in locked rooms, tended to by (mostly) trusted staff, and malicious acts were harder and could not cascade
- Remote-access terminals multiplied attack surface
- Internetworking multiplied attack surface and added system-wide risks

What is Winning, Anyway?

A System-Wide Offense Advantage Is Far More Than Just Simplicities Like
"The Attacker Only Has to Be Right Once..."

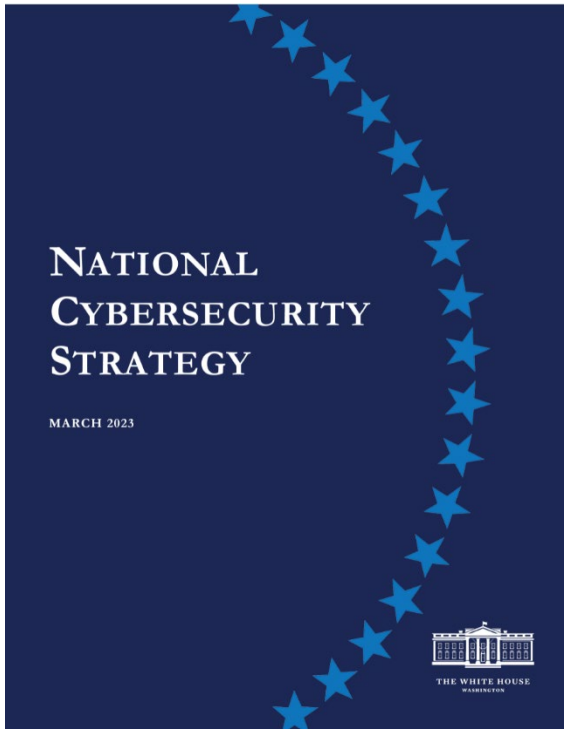
1. Internet was never designed for security
2. Internetworking both increased attack surface and allowed global access
3. Software is shipped insecurely by design and default
4. Countless single points of failure and common mode vulnerabilities exist
5. Cyberspace is tightly connected and highly interdependent; many failure modes are only obvious in retrospect; and it is prone to unpredictable, cascading failures



Defensibility and Resilience: A New National Goal

"We must make fundamental changes to the underlying dynamics of the digital ecosystem**, shifting the advantage to its defenders and perpetually frustrating the forces that would threaten it**."

"Maintaining an open, free, global, interoperable, reliable, and secure Internet and building a **more defensible and resilient digital ecosystem** will require generational investments by the federal government, allies and partners, and by the private sector."



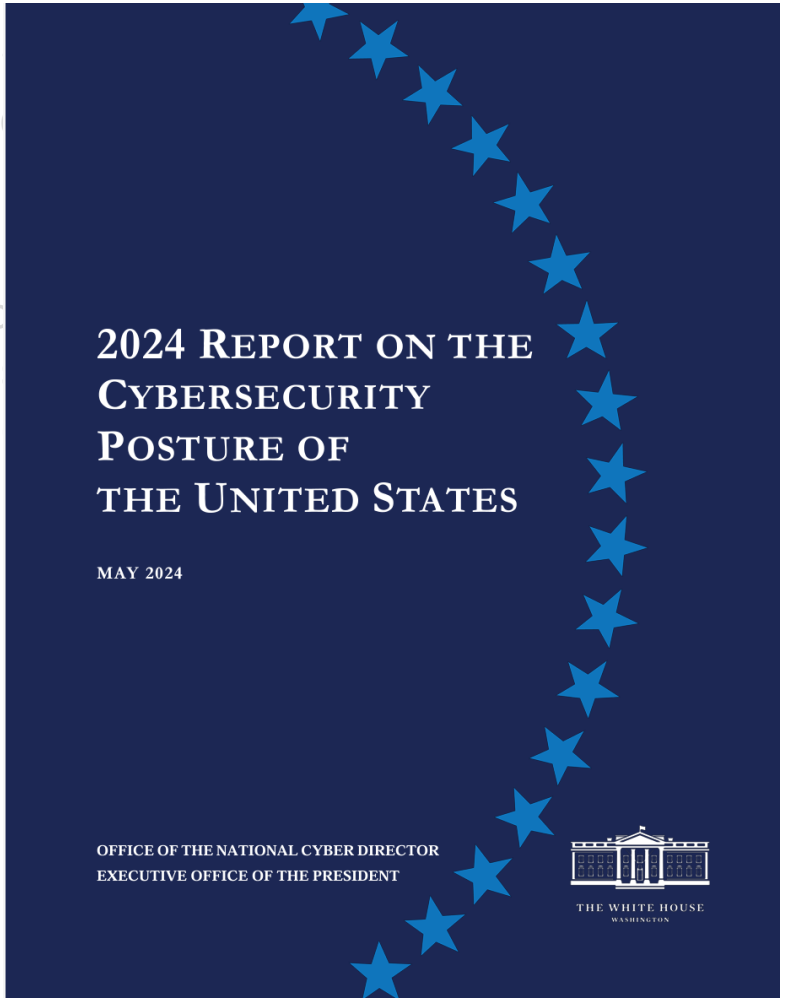
(Source: The White House. "National Cybersecurity Strategy." Washington, DC, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf, 1 March 2023.)

Goal D>O

Defensibility and Resilience: A New National Goal

- "We must make fundamental changes to
  ecosystem**, shifting the advantage to its**
  the forces that would threaten it."

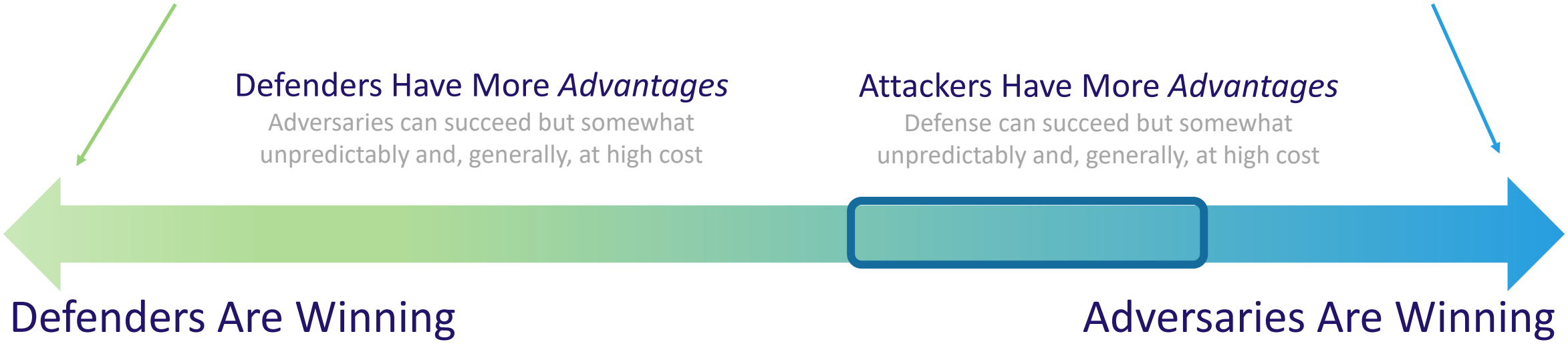
- "Maintaining an open, free, global, interc
  and building a **more defensible and re**
  generational investments by the Federal G
  the private sector."


2024 REPORT ON THE CYBERSECURITY POSTURE OF THE UNITED STATES
MAY 2024
OFFICE OF THE NATIONAL CYBER DIRECTOR
EXECUTIVE OFFICE OF THE PRESIDENT
THE WHITE HOUSE
WASHINGTON

Goal D>O

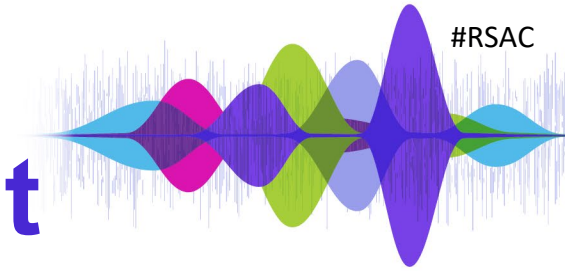
(Source: Office of the National Cyber Director. 2024 Report on the Cybersecurity Posture of the United States. https://www.whitehouse.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf, Washington, DC, May 2024.)

Defensibility and Resilience: A New National Goal


Defenders Have *Supremacy*
Adversaries have tremendous difficulty achieving even simple goals against poorly resourced organizations
Attackers Have *Supremacy*
Even advanced defenders struggle to prevent basic attacks and threat attackers from achieving substantial impact
Defenders Have More *Advantages*
Adversaries can succeed but somewhat unpredictably and, generally, at high cost
Attackers Have More *Advantages*
Defense can succeed but somewhat unpredictably and, generally, at high cost
Defenders Are Winning
Adversaries Are Winning

"Winning" means sliding left, every week, month, year

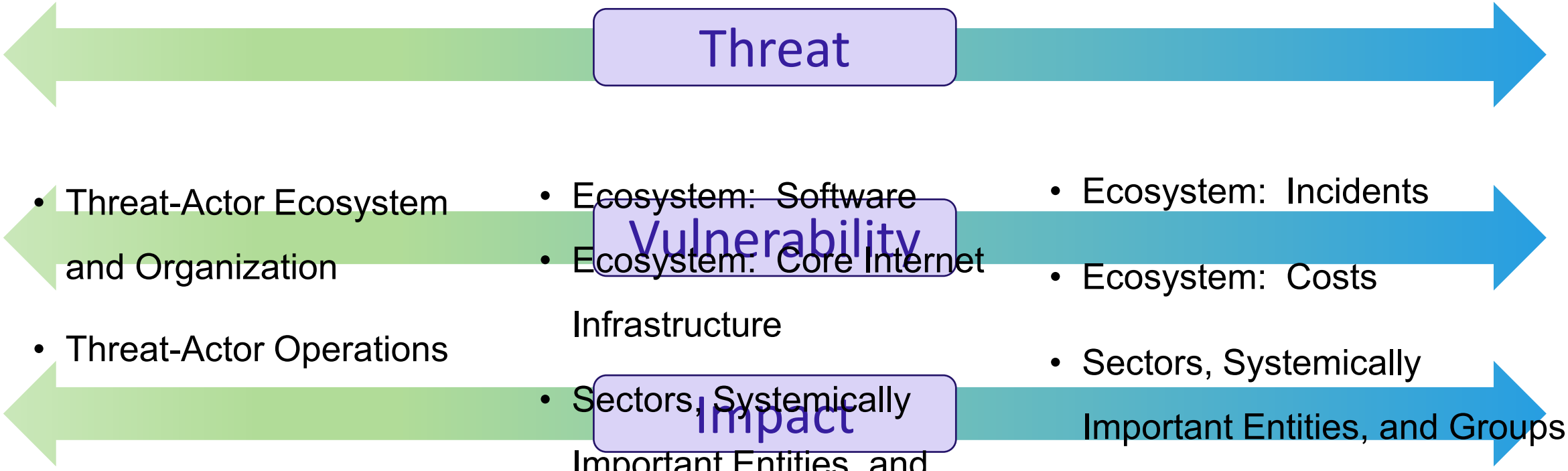
So Many Metrics…
But Little System-Wide Insight



- Many metrics are *useless*
- Others track inputs or outputs, not *outcomes*
- Most are optimized for those with *purchase authority*
- A few are *perfect* (MTTD)

- Others are close but not quite… such as *not in time series*
- No framework how metrics interact to understand the full story

One Way to Tackle This…

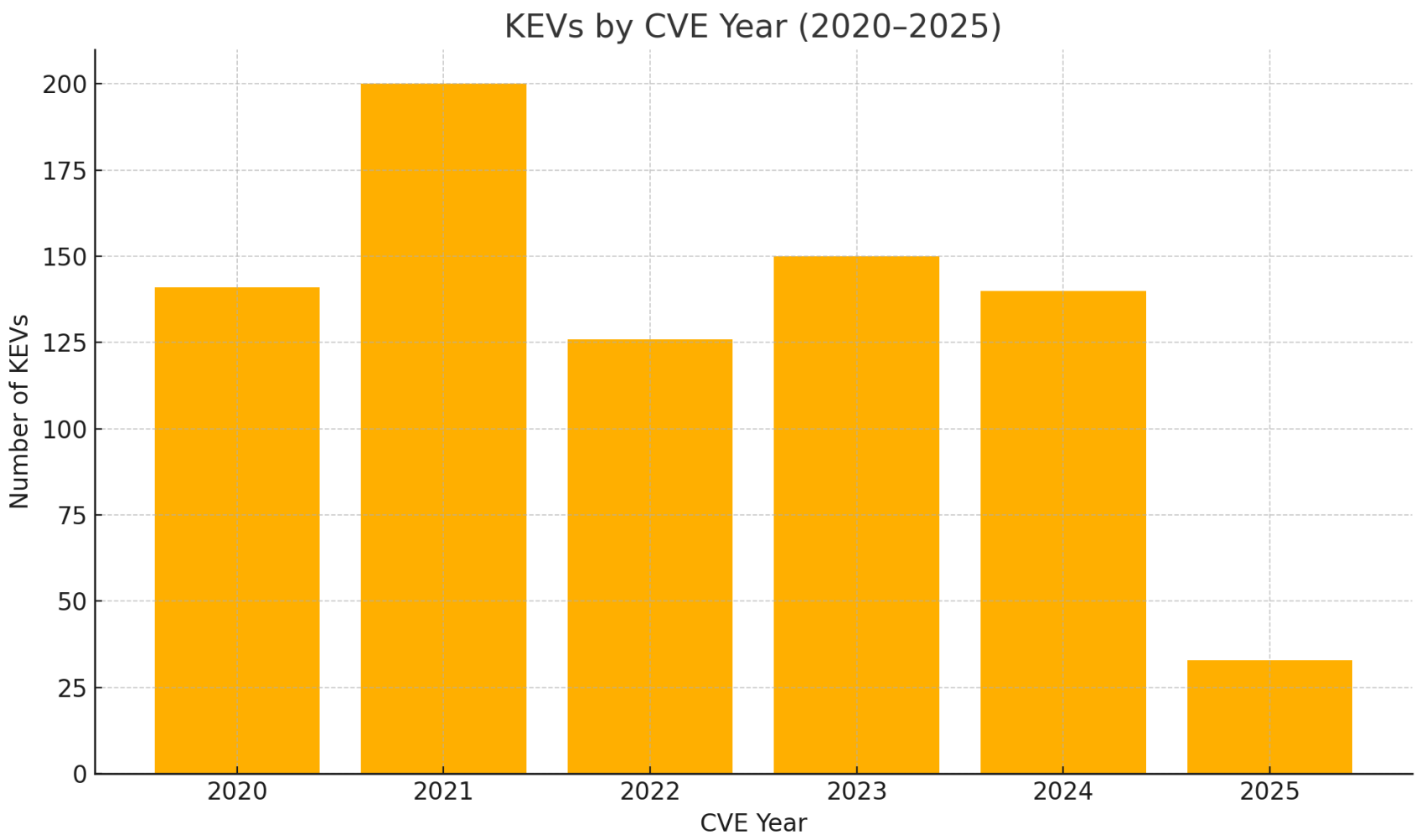


RSAC™ 2025 Conference

How are we doing on software according to the data?

Many Voices.
One Community.

Known Exploitable Vulns by Year of CVE

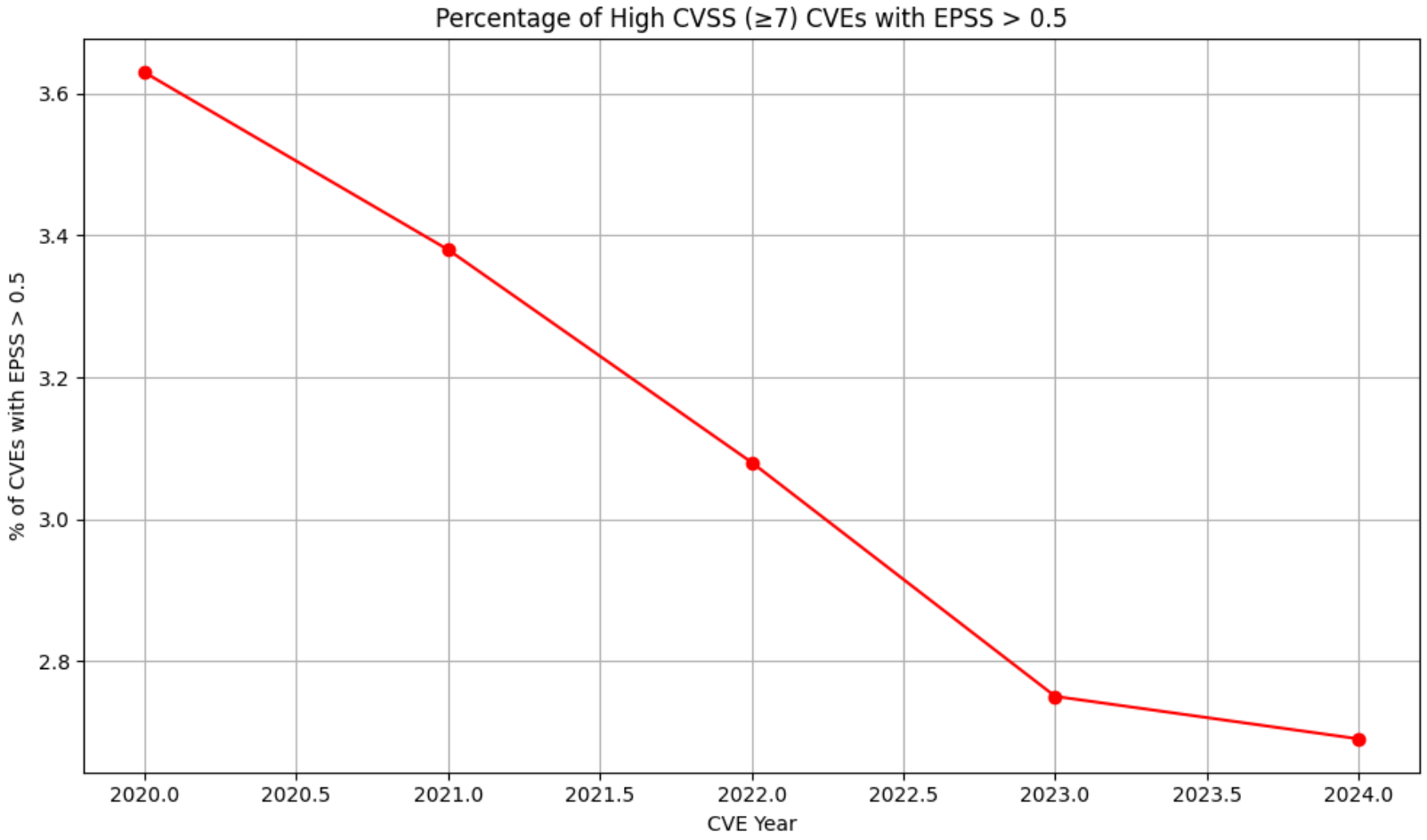


Known Exploited Vulnerabilities Catalog

33 KEVs in 1st quarter 2025 gives 132 prorated annually

Data source: https://www.cisa.gov/sites/default/files/csv/known_exploited_vulnerabilities.csv

Using EPSS to see if CVEs are becoming less exploitable



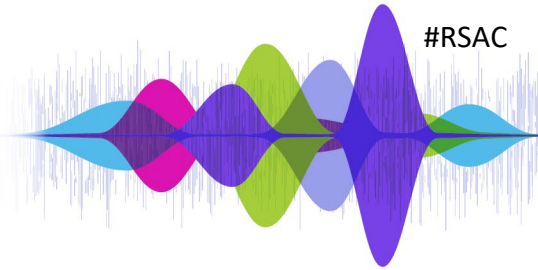
EPSS
Exploit Prediction Scoring System

Data source: https://epss.empiricalsecurity.com/epss_scores-current.csv.gz

Data at the code level

https://www.veracode.com/blog/state-of-software-security-maturity-2025/

Data comes from Veracode AST findings

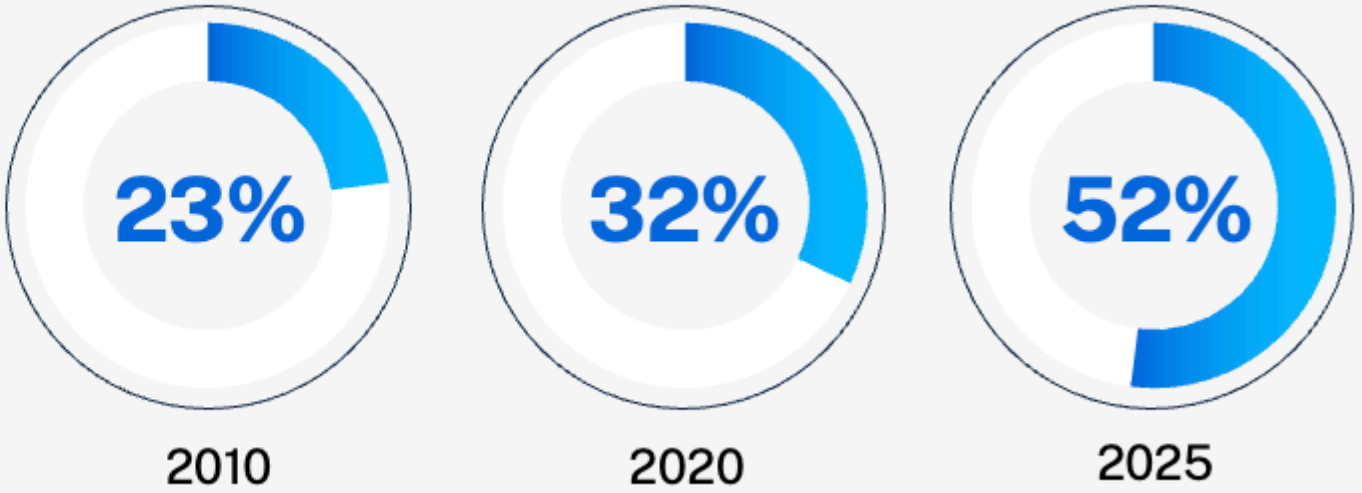


- **1.3M unique applications with 126.4M raw findings**
- **107.4M findings identified via SAST scans**
- **3.9M findings identified via DAST scans**
- **15M findings identified via Software Composition Analysis**

This data represents companies of all sizes, commercial software suppliers, software outsourcers, and open-source projects. In most analyses, an application was counted only once, even if it was submitted multiple times as vulnerabilities were remediated, and new versions were uploaded. For software composition analysis, each application is examined for third-party library information and dependencies. The library dependencies are checked against a database of known flaws.

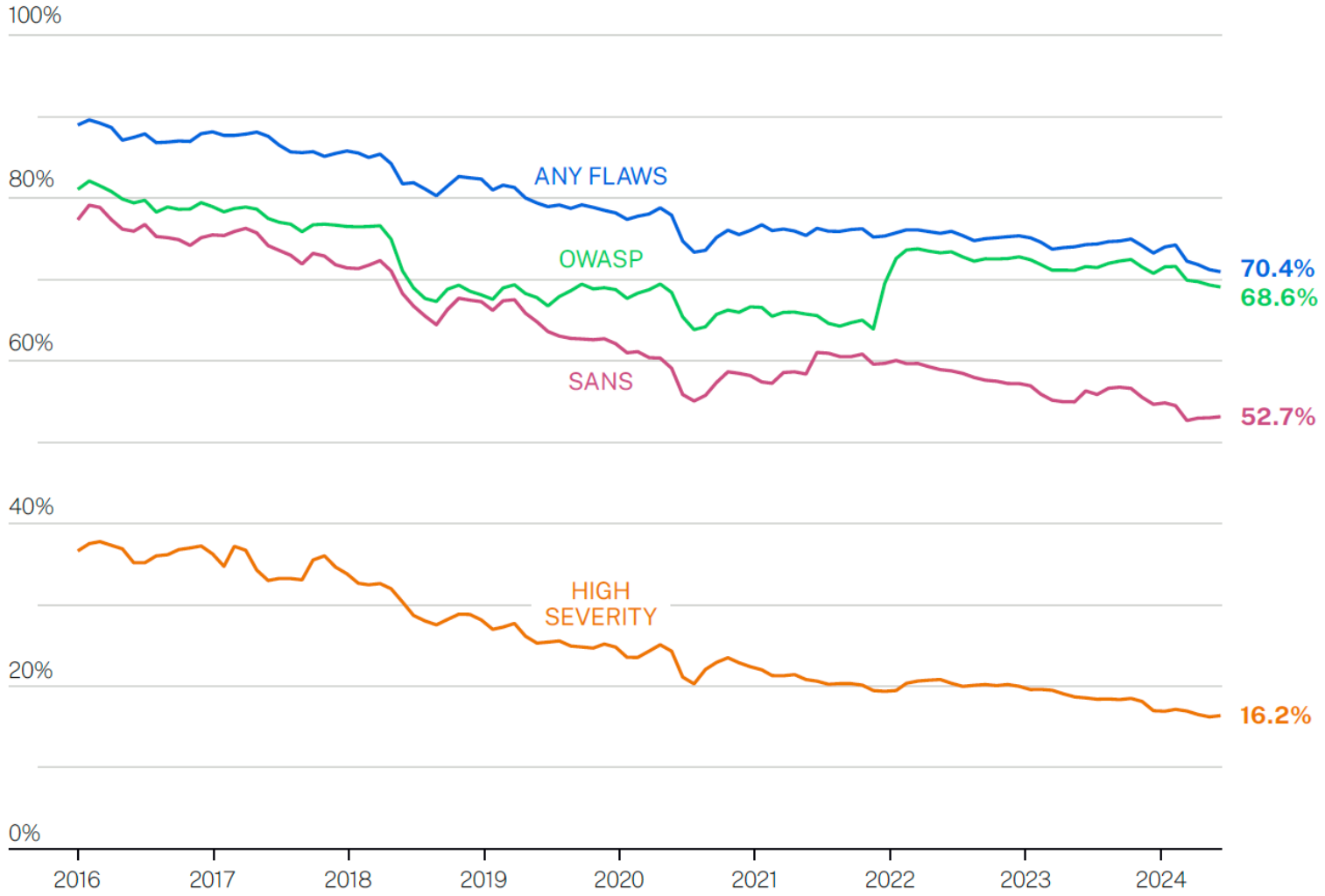
The Good News

The percentage of apps **passing the OWASP Top 10 has increased 63%** in 5 years (from 32% to 52%) and **126%** in 15 years (from 23% to 52%).



1st and 3rd party code vulnerabilities based on SAST, DAST, and SCA findings

Prevalence of security flaws over time (SAST only)



The Bad News

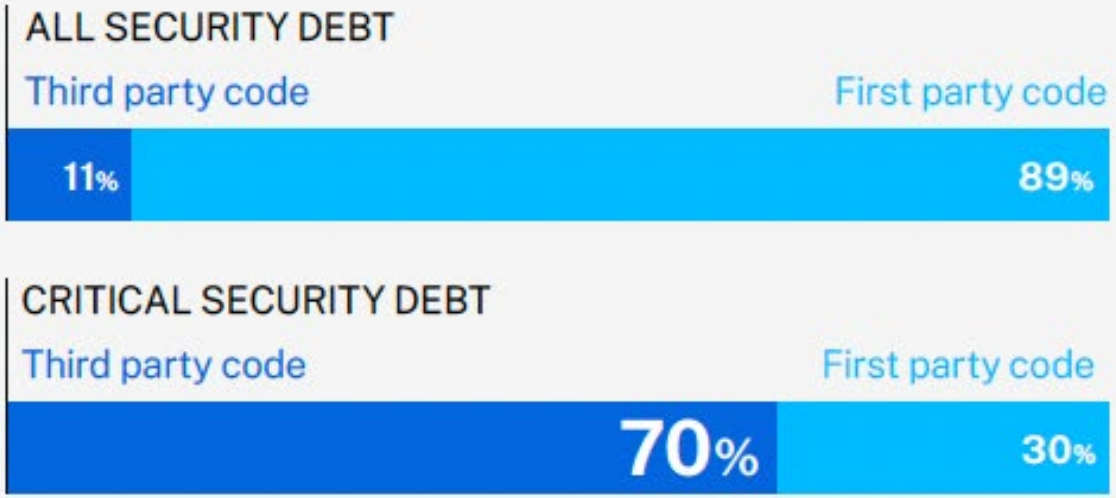
The average number of days to fix flaws has increased 47% in 5 years (from 171 to 252 days) and **327%** in 15 years (from 59 to 252 days).

1st and 3rd party code vulnerabilities based on SAST, DAST, and SCA findings

And fixing slow leads to…

Half of organizations have critical security debt (high severity, high exploitability)...

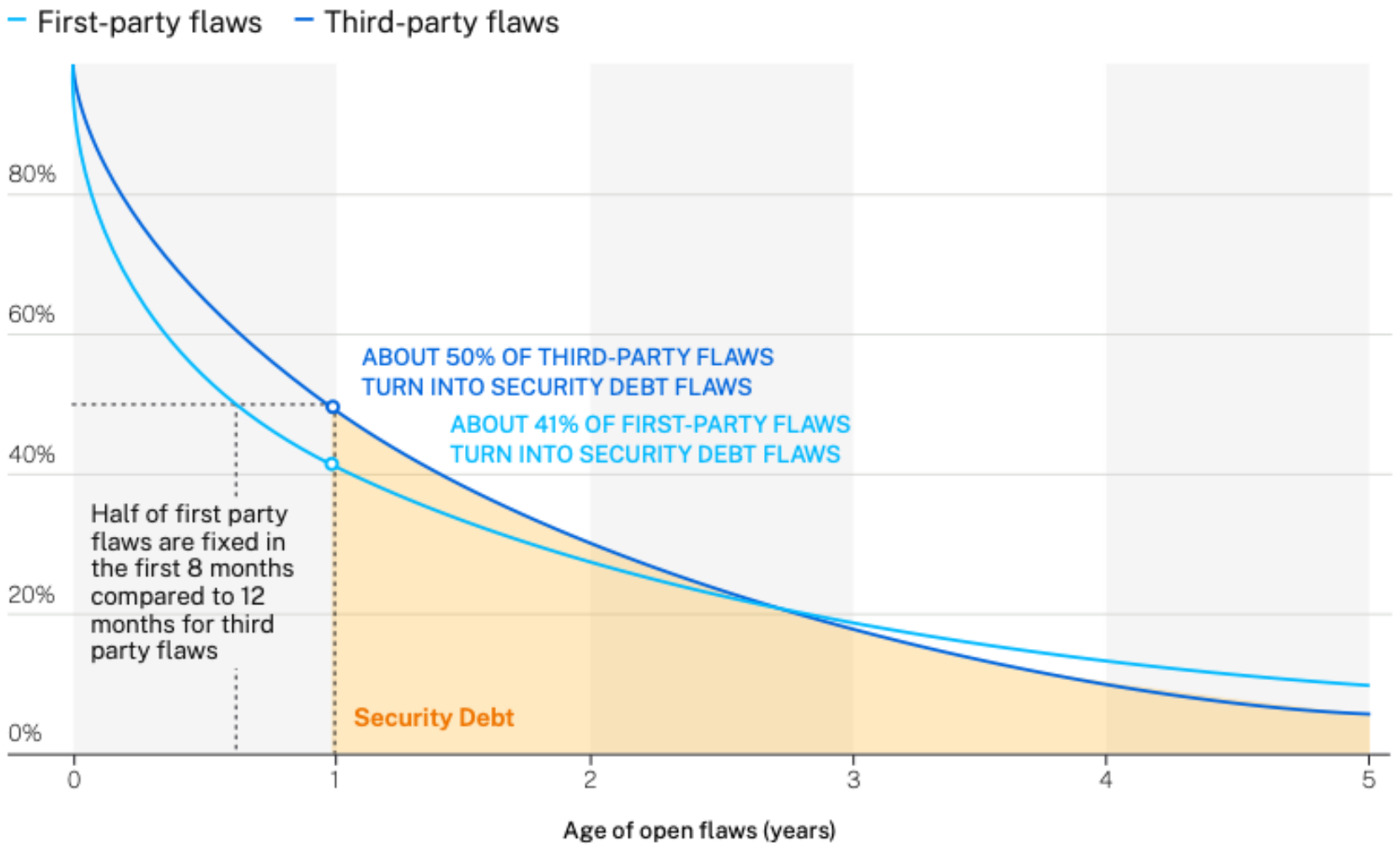
...and 70% of it comes from third party code and the software supply chain.



Flaw remediation time by language

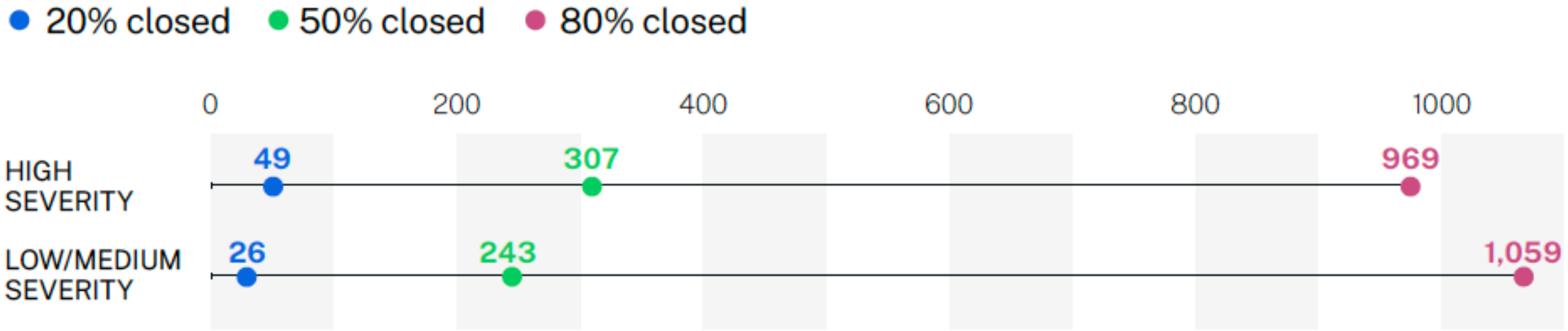
FIGURE 25

Comparison of remediation timelines for first-party vs. third-party code

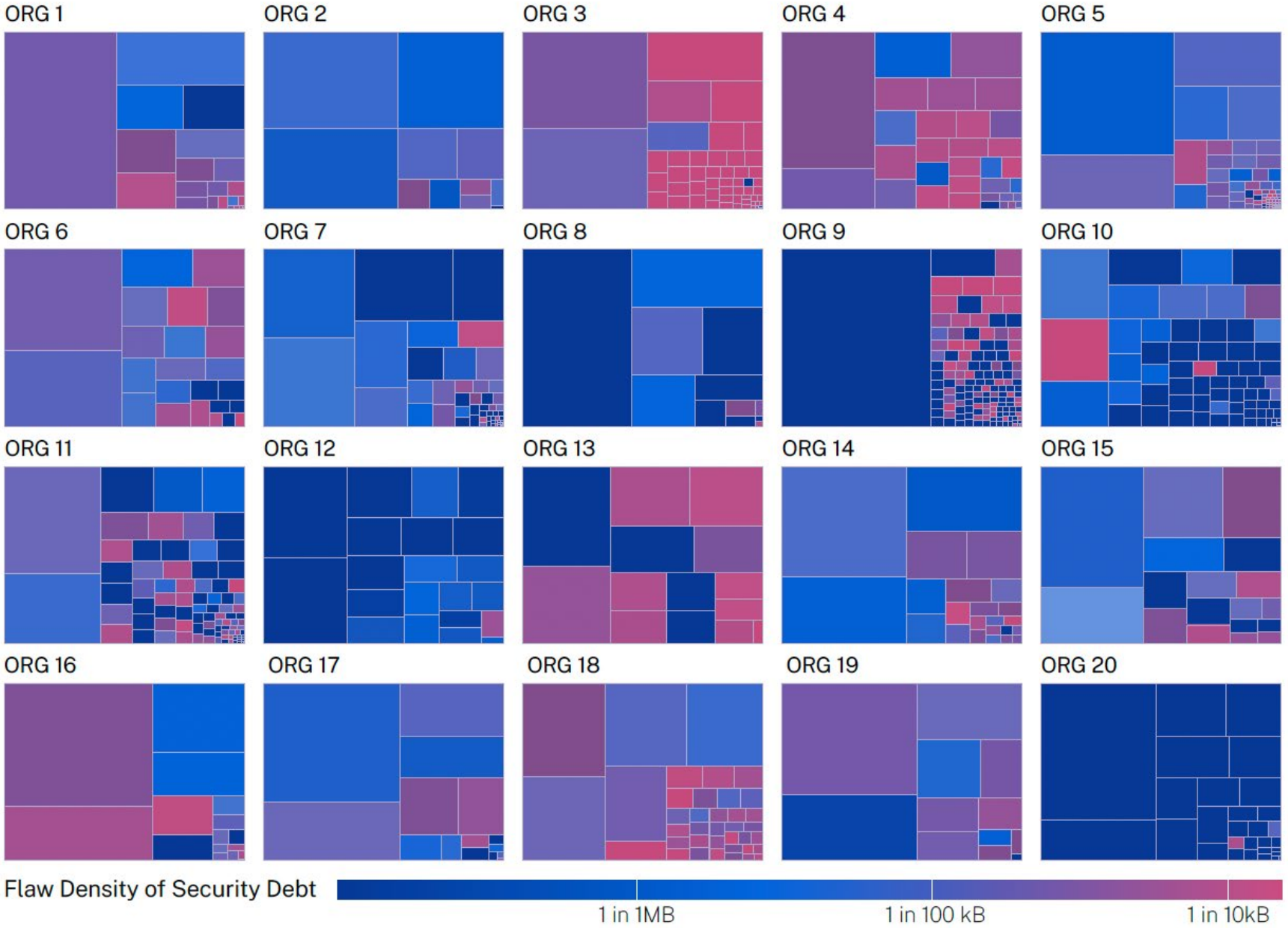


NOTE: Open source flaws come in two types of dependencies: direct and transitive. When your configuration file references a library, it's considered a direct dependency. If those direct dependencies depend on other libraries, they're transitive. Direct dependencies are the easiest to fix. Things get trickier with transitive dependencies; it may be that a fix will break some functionality in the direct library, meaning a slower and more difficult fix process. In some cases there will be code refactoring which takes more time.

Flaw remediation time by severity



Distribution of security debt across applications in 20 example organizations



Secure apps are here. They are just not very evenly distributed.

	Leading organizations	Lagging organizations
FLAW PREVALENCE	Below 43%	86% or more
FIX CAPACITY	Above 10% of flaws monthly	<1% of flaws monthly
FIX SPEED	Half of flaws in 5 weeks	Half of flaws in over a year
SECURITY DEBT	<17% of apps	>67% of apps
OPEN-SOURCE CRITICAL DEBT	<15% critical debt from open-source	100% critical debt from open-source

Data from Cobalt State of Pentesting Report 2025

- The proportion of serious findings in pentests has declined by about half (from 20% to 11%) over 10 years, demonstrating the positive impact of "shift left" security programs.
- However, this progress appears to have plateaued. When we look at the rate for serious findings being resolved in each calendar year, it remains stuck at just 55%.
- Larger organizations take over a month longer than smaller ones to resolve serious issues (61 days to 27 days).
- 57% of organizations resolve at least 90% of their serious findings (whereas another 15% of orgs resolve 10% or less).

Source: https://www.cobalt.io/blog/key-takeaways-state-of-pentesting-report-2025

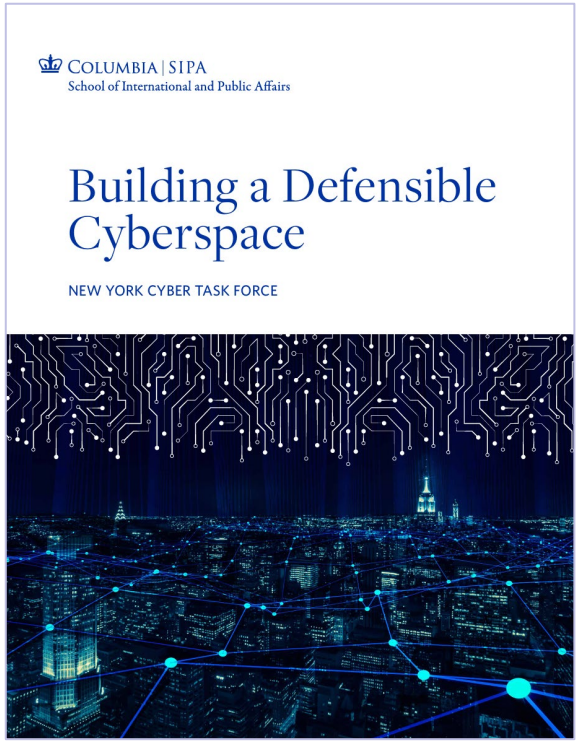
RSAC 2025 Conference

Recommendations

And the way ahead

Many Voices.
One Community.

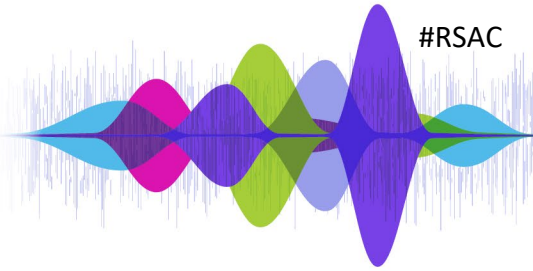
For Further Reading



LAWFARE
Topics
Podcasts & Multimedia
Projects & Series
Resources
About
Cybersecurity & Tech
Measuring Policy Effectiveness of Cyber Defensibility and Deterrence
Jason Healey | Tuesday, September 10, 2024, 12:00 PM
Share On:
The United States needs better ways to understand success in cyberspace. Doing so is now within reach, with the right, top-down approach.

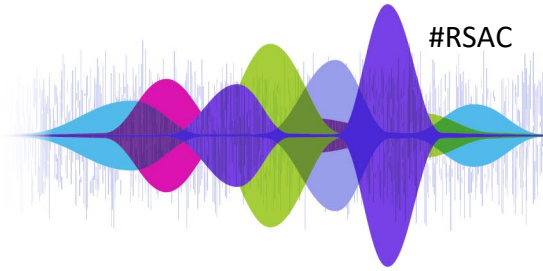
America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE
Search
Topics
Spotlight
Resources & Tools
News & Events
Careers
About
National Council of Statewide Interoperability Coordinators
Home / Topics / Cybersecurity Best Practices / Secure by Design
SHARE:
Secure by Design
It's time to build cybersecurity into the design and manufacture of technology products.
SECURE BY DESIGN

Recommendations for Government Policy



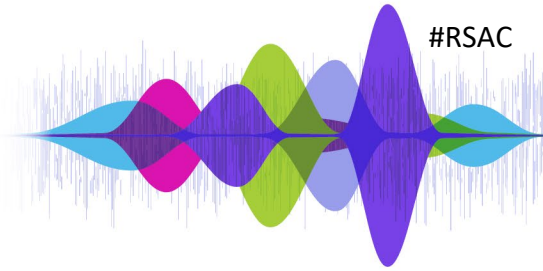
- Don’t give up on defense!
  - Learn from the actual data from authoritative sources like SoSS
  - Encourage cybersecurity companies (and others with data) to report defensibility-relevant statistics in time-series, mapped to the catalog
  - Fund and develop a framework across threat, vulnerability, and impact
  - Produce an annual report on if defenders are winning

Recommendations for Software Producers



- Yes, do Secure by Design!
- Benchmark your AppSec program. How long does it take for your teams to fix? Work with product management and engineering to get fix capacity so you can fix 10% monthly
- If can't spare capacity to fix 10% monthly, then you must prioritize based on severity and exploitability
- Hold *your* vendors accountable and expect regulators and customers to hold *you* accountable.

Winning Is Possible!



- Most of us got into this field to make a difference; we are, but mostly only at small scale
- There are signs of progress, just look at key findings from years of SoSS and Cobalt State of Pentesting
- But, we need more information, reported to a common framework, in time series
- **Keep in mind the end goal to shift the balance towards defender, so our grandkids aren't facing the same problem**

RSAC™ | 2025 Conference

Many Voices.
One Community.

Sign up for Columbia’s new cyber-regulation newsletter

RSAC™ 2025 Conference

Many Voices.
One Community.